REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested.

The Abstract and specification have been amended to put them into appropriate US format as required.

The outstanding rejection of claim 3 under 35 U.S.C. §112, second paragraph, has been mooted by the cancellation of this claim and the re-drafting of original claims 1-12 into more traditional US format as new claims 13-24 which correspond respectively to original claims 1-12.

The rejection of claims 1-12 under 35 U.S.C. §102 as allegedly anticipated by Srisuresh et al. '431 is respectfully traversed.

In a nutshell, Srisuresh '431 cannot possibly anticipate applicant's claims because the destination address is not altered on the outbound phase. The Examiner's allegations to the contrary actually refer only to modifications of the destination address for reply (i.e., the inbound phase). In other words, the only actual address altered corresponds to the source of the original outbound message in Srisuresh '431.

The contrast with the applicant's claimed invention where both the source and the destination addresses on both the outbound and the inbound phases are modified. In particular, the applicant's invention considers issues related to load balancing where the outbound destination address may be modified by the network management scheme re-directing outbound data grams in an IP network to balance the load of various network elements. Many applications are sensitive to the reply message having a different source address from the original destination address. In such applications, unless the source address for the reply matches the original

(outbound) address of the original intended destination, an error data occurs. The applicant's invention seeks to avoid such error states by insulating the originating application from any source/destination address changes caused by network management scheme, load-balancing measures.

The Examiner's attention is drawn to the following attached materials and PTO-1449 (for which the IDS fee appropriate to this stage of prosecution is also concurrently paid):

i) a copy of the International Examination Report (and each newly cited reference therein); and

ii) a copy of a recently issued EPO Examination Report contents for the European counterpart to this application.

Official consideration and citation of all of this additional material is respectfully requested.

As the Examiner will note, reference D5 relied upon in the EPO may be more relevant than Srisuresh '431.

Independent claims 1, 6, 11 and 12 (now cancelled without prejudice or disclaimer) have been amended to new claims 13, 18, 23 and 24 respectively.

Method claim 13 is directed to a method of transparently re-routing data elements transmitted during a network connection (see page 10, final paragraph for support), and is further limited by the additional feature that the network connection has protocols above the transport layer protocol capable of maintaining data transmission during disconnection and reconnection when the data elements are re-routed (see page 11, 2nd paragraph for support), and by said first

point of interception differing from said original destination address (see page 11, 3rd paragraph, 3rd sentence, and Figure 3 generally).

Apparatus claim 18 has been amended analogously. Claims 23 and 24 have been amended to independent form and include the features previously recited by reference to independent claims 1 (now 13) and 6 (now 18) respectively.

The Examiner has alleged that Srisuresh '431 discloses an original sources 10.0.0.5 and an alternative source 198.76.29.1 and describes modifying the original destination address to an alternative destination address (column 6, lines 1-3: Srisuresh discloses an original designation address = 198.76.28.4 and an alternative destination address 198.76.29.1).

Respectfully, column 6, lines 1-3 of Srisuresh only states: If a reply should come back (i.e., inbound), then it would contain a source address 198.76.28.4 (the source address of the reply being the destination address of the outbound packet) and a destination address of 198.76.29.1. This is shown by arrow (c) in Figure 2.

Accordingly, claim 13 is not anticipated by Srisuresh (nor was original claim 1), as the destination address is changed outbound to an alternative destination address and as the original source address is also changed at the same point.

Nothing in Srisuresh indicates that if the destination address in the outbound phase is changed, then in any reply, the source address for the reply (which corresponds to the changed destination address) will also need to be changed. This is because nothing in Srisuresh considers the stability of the applications receiving the reply, or considers that if they receive a reply with a changed source address, this may cause an error state to occur.

Claim 13 distinguishes more clearly the features of the invention from RFC 2391: "LOAD SHARING USING IP NETWORK ADDRESS TRANSLATION (LSNAT)", August 1998 (hereinafter referred to as D5 – the designation used in the parallel EPO proceedings). The remaining independent claims also have been amended where appropriate.

D5 can be summarized as describing load sharing using network address translators in which a client attempts to access a server and is diverted to another server represented by a server virtual address (a globally unique IP address that identifies a physical server or a group of servers that provide the same or similar functionality). D5 describes a LS-NAPT load sharing with no topological constraints on the servers in which the LS-NAPT router provides an interface address which replaces the address of the virtual server.

An example is shown in Figure 3 of D5 in which the virtual server address S (172.87.0.100) is the same as the address of the WAN link and the LS-NAPT serveris enabled on the WAN interface. It is very clear from D5 that when a client (source address 198.76.29.7) initiates an HTTP session, this is done to the virtual server address S which is now the same as the LS-NAPT address – i.e., to 172.87.0.100. There is therefore no "interception" at the LS-NAPT server – the client packets are directed directly towards it, so the original destination of the client packets is the same address as the server implementing the load-balancing in D5.

Furthermore, in D5 specific resources on the LS-NAPT server are occupied by the load-balancing and once a session has been assigned a host, the session cannot be moved to a different host until the end of that session. This means loads cannot be switched between hosts in the midst of sessions. This is made very clear on page 3, 1st paragraph, lines 4 to 10 of D5.

In contrast, it is clear from applicant's Figures 1 and 3 of the drawings and from the specification (for example, see page 8, last paragraph and page 11, 3rd paragraph 2nd sentence) that the proxy server 123 intercepts packets according to an exemplary embodiment of invention to re-route them during a network connection. The packets are not addressed directly to the proxy server, instead the proxy server of this exemplary embodiment intercepts packets and then performs a look up operation to determine if the destination address is a diverted address. There is no need to specify virtual server addresses to the proxy server. To ensure that the process is transparent, the proxy server changes not just the destination address to the diverted address but also the originating address to the address of the proxy server. The proxy server may or may not receive all the packets addressed to the specific destination address by the server.

By also changing the originating address to the address of the proxy server, when the packet destination address is changed, the process is made transparent in that those packets which are diverted to the other server and causing or providing return packets, will cause packets to be returned to the originating proxy server which can then replace the apparent source address with the original client source address by performing another look-up process.

There is no need to specify a virtual server address in the packet header, nor is there any need for an interface on the proxy server to assume the virtual server address. Moreover, the addresses to which any individual packet received is diverted can be determined dynamically in real-time. Accordingly, it is not necessary for a packet to be aware of the presence of the proxy server in advance of requesting a session with a destination server or to be provided with any "virtual server address" information. The amount of information which needs to be processed by the proxy server and stored is therefore limited to re-direction pairs.

By providing a proxy server with the capability to update the divert address of packets stored as current connections in the address table store of the proxy server, in a network connection (i.e., during a session) packets can be redirected transparently while the network connection is still ongoing. For example, see page 10, final paragraph to page 11, 2nd paragraph. This is done by the proxy server 205 updating the appropriate entry in the diverted address section 209 and searching the content of the current connections section 211 of the address table 207 and updating the appropriate diversion address information.

A skilled but unimaginative person, faced with the objective problem of how to divert traffic from one destination to an alternative destination even during a network connection would, on reading the teachings of D5, understand only that packets need to specify a virtual server address, which can be the same as an interface on a load-balancing router (see page 10 of D5 "datagrams from clients are forced to bear the address of the LS-NAPT router as the destination address"). This in fact therefore introduces a load-imbalance, as data has to be specifically routed to LS-NAPT server before it can be redirected. They would also learn from page 3, paragraphs 1 of D5 that once a session has been assigned a host, the session cannot be moved to a different host until the end of that session.

D5 does not consider that if a client sends packets to an address which is determined by a network monitor to be overloaded, then providing a proxy server is able to intercept one or more or all packets and check if the destination address can be changed using a lookup table to a divert address, it is possible for the network connection to be maintained providing the protocols above the transport layer support this.

Nor does D5 teach providing a server which diverts addresses under the direction of a network monitor function (rather than based on the servers determined by the global server address provided by the client). In particular, nothing in D5 teaches providing a network monitor which can send instructions to the proxy server using different ports from that used for sending and receiving data to/from the client and server, which means the network monitor function can update the divert address in real-time, even during an ongoing network connection.

Accordingly, it is submitted that the applicant's claims are both novel and inventive over the cited prior art D5, in that they specifically require the provision of a proxy server transparently re-routing intercepted data packets which advantageously removes any need for the packets to carry virtual server address information or to be explicitly directed initially to the router.

Accordingly, this entire application is now believed to be in allowable condition and a formal Notice to that effect is respectfully solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: Larry S. Nixon

Larry S. Nixon
Reg. No. 25,640

LSN:vc
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100